CASE STUDY: SECURE DEPLOYMENT OF AUTONOMOUS HAULAGE SYSTEMS

This case study was developed based on a presentation from a member mining company, at the December 2021 MM-ISAC Conference on Cyber Resiliency.

EXECUTIVE SUMMARY

This case study covers autonomous haulage systems and the security measures and risks associated with their deployment. Although these systems improve personnel safety and operational efficiencies, there are cybersecurity challenges because all operational assets in the mine are connected.

Autonomous haulage system security needs to be designed alongside its implementation because of the evolving threat landscapes and cybersecurity attacks. Key risk management concepts for securing these systems effectively include:

- Establishing impact: Operational technology (OT) dependencies and loss
- Vulnerabilities: Exposure and attack pathways
- Threats: Threat modelling
- Assessing Risk: Likelihood (frequency)
- Risk Treatment: Accept or mitigate and apply controls

The MM-SIAC Working Group has created a risk assessment process that covers autonomous haulage system controls. Some of these controls include:

- OT and information technology (IT) integration
- Third-party/original equipment manufacturer (OEM)
- Access and authorization
- Wireless
- Vulnerability management and endpoint protection

TABLE OF CONTENTS

1. INTRODUCTION

This case study describes some of the work and key learnings from the Mining and Metals Information Sharing and Analysis Centre (MM-ISAC) AHS Security Working Group on securing autonomous haulage systems. Certain additional details are provided from the experience of applying the working group guidance as it was applied at the operation. Autonomous haulage systems are defined as conventional haul trucks outfitted with operational technology (OT) provided by the OEM that allows for safe unmanned operation. These systems use traditional wired and wireless networks, virtual infrastructure, servers, and control centres composed of regular desktop workstations.

OT is a hardware with a digital component that is programmed to interact with industrial elements, such as processes, assets, and equipment, to control or detect changes. This is done by using direct control and monitoring capabilities. Examples of these equipment include wireless high precision GPS devices used heavily for open pit fleet management and industrial control systems used for controlling processes in mills, refineries, and ports. Practically every aspect of mining from pit to port has a dependency on OT.

2. HOW IS OPERATIONAL TECHNOLOGY SECURITY DIFFERENT?

Securing OT systems differs from securing IT systems because OT security is more focused on protecting operational assets and supporting safe production instead of protecting the data (Figure 1).

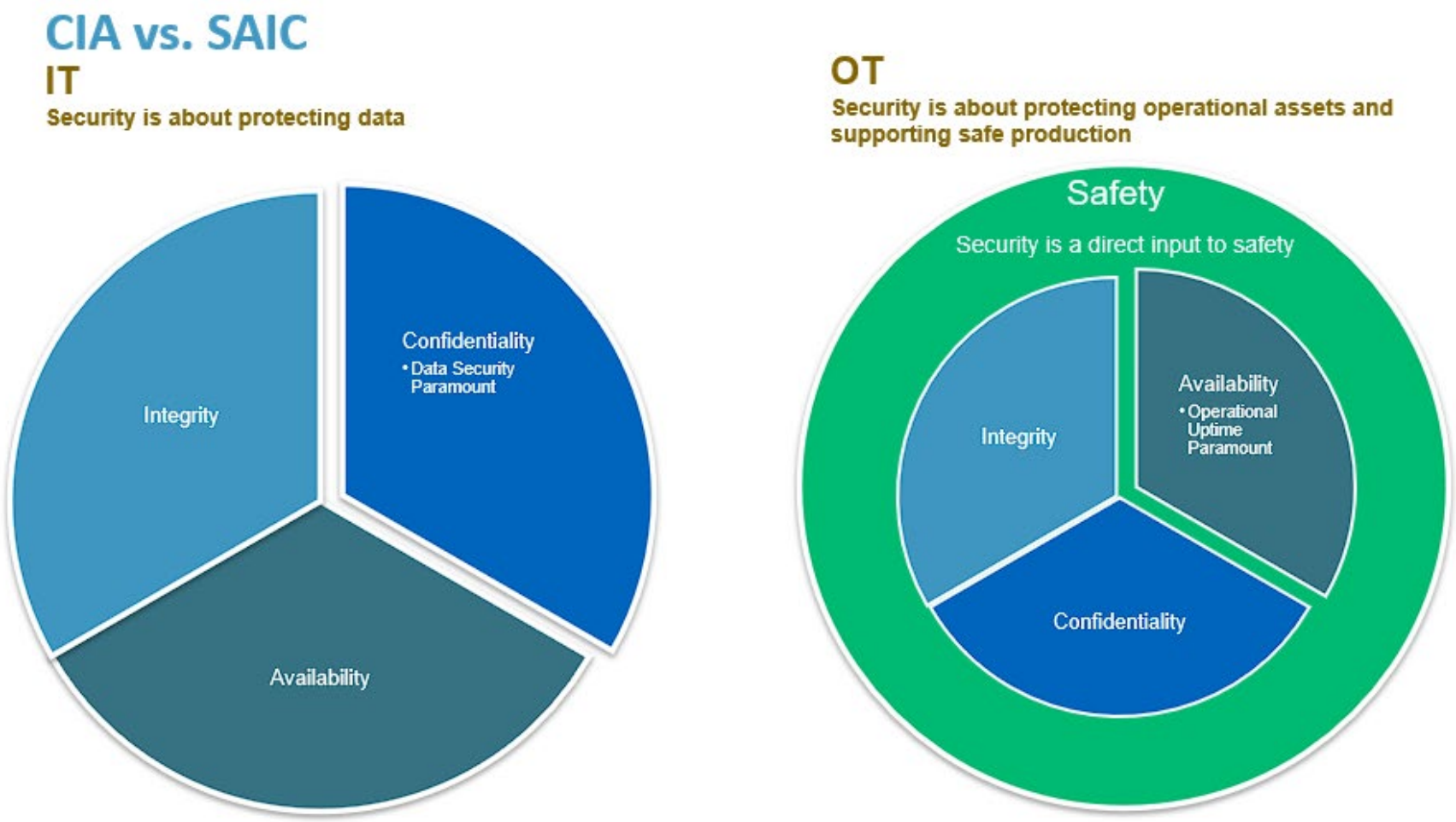


Figure 1. IT and OT Security Comparison

3. WHAT IS AHS AND WHY DOES IT MATTER?

Autonomous haulage systems (AHS) are conventional haul trucks outfitted with OEM-provided operational technology that allows for safe unmanned operation. This autonomous system utilizes traditional wired and wireless networks, virtual infrastructure, servers, along with a control center composed of regular desktop workstations. High precision GPS systems provide all mobile vehicles used in the autonomous system accuracy to 1 cm precision. Safety systems such as lidar and radar systems provide obstacle detection and collision avoidance to the onboard supervisory logic that governs the vehicle and allows integrations with other mine vehicles such as light trucks, dozers, and loaders. Operators monitor autonomous haulage system status information and send vehicle route following commands while field operators update vehicle route information for changes in the mining environment, such as a broken-down vehicle or rock debris on haul roads.

Additional considerations include:

- Autonomous haulage systems have a heightened risk profile when compared to traditional conventional vehicle operations.
- These systems have total reliance on wireless technologies for safe production and operational control.
- Digital transformation within the mining industry has established rich connectivity to OT networks from enterprise systems.
- Existing relevant standards focus on safety, but cybersecurity is a minor consideration. These standards typically revolve around mitigating risks for personnel and functional safety; however, cyber-physical risks are briefly covered.

4. THE MM-ISAC AUTONOMOUS HAULAGE SYSTEMS WORKING GROUP

The MM-ISAC Autonomous Haulage Systems Working Group has created a risk assessment process for members, complete with controls and mitigations guidance to help with the design process. The group has been working to:

- Employ system-level threat modelling and risk analysis
- Derive security guidance from threat modelling data set
- Create actionable security recommendations for both operators and OEMs
- Align existing safety-focused autonomous haulage system standards to cybersecurity standards (see Figure 2)

Additionally, there are plans to add a private LTE to attack pathways and update threat models.

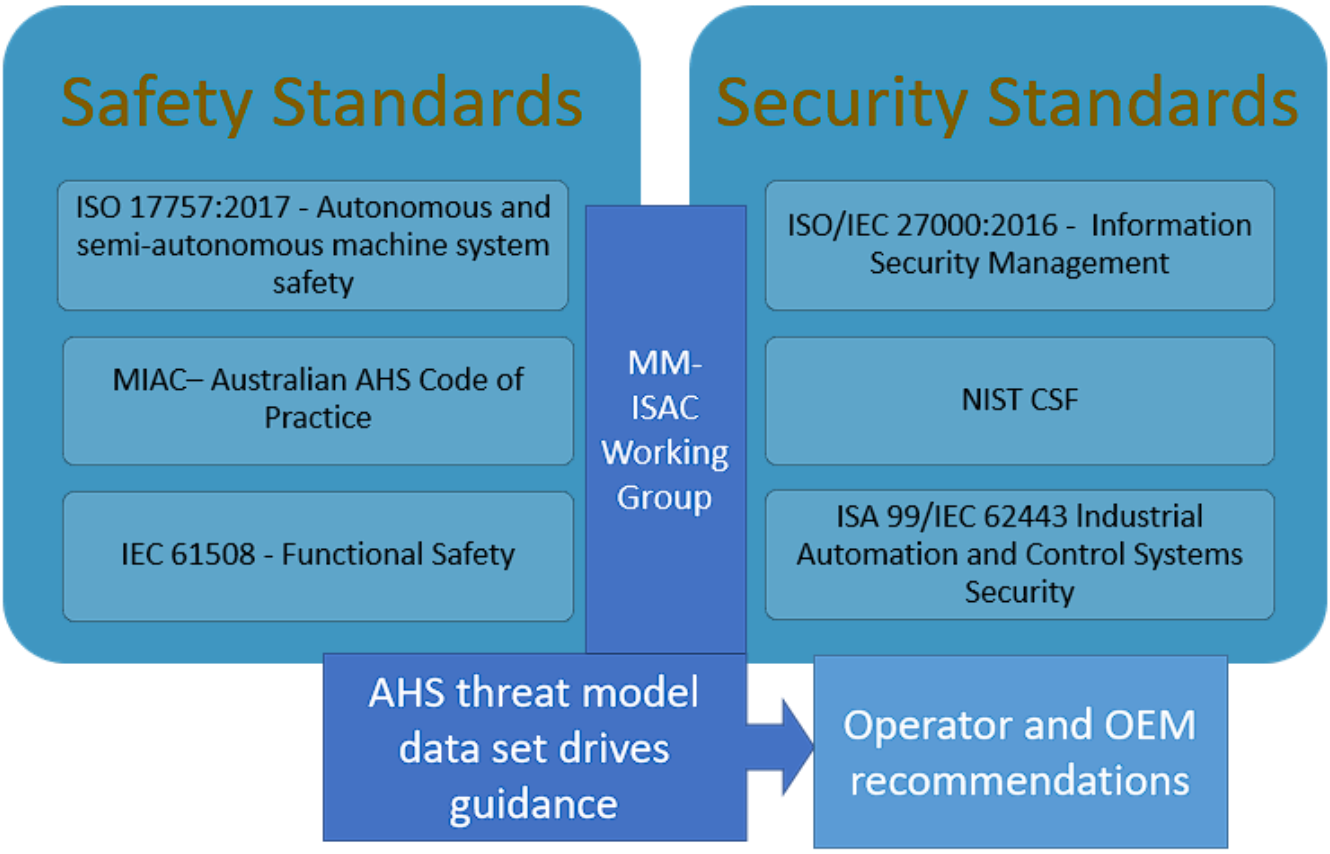


Figure 2. MM-ISAC Autonomous Haulage System Working Group and Existing Standards

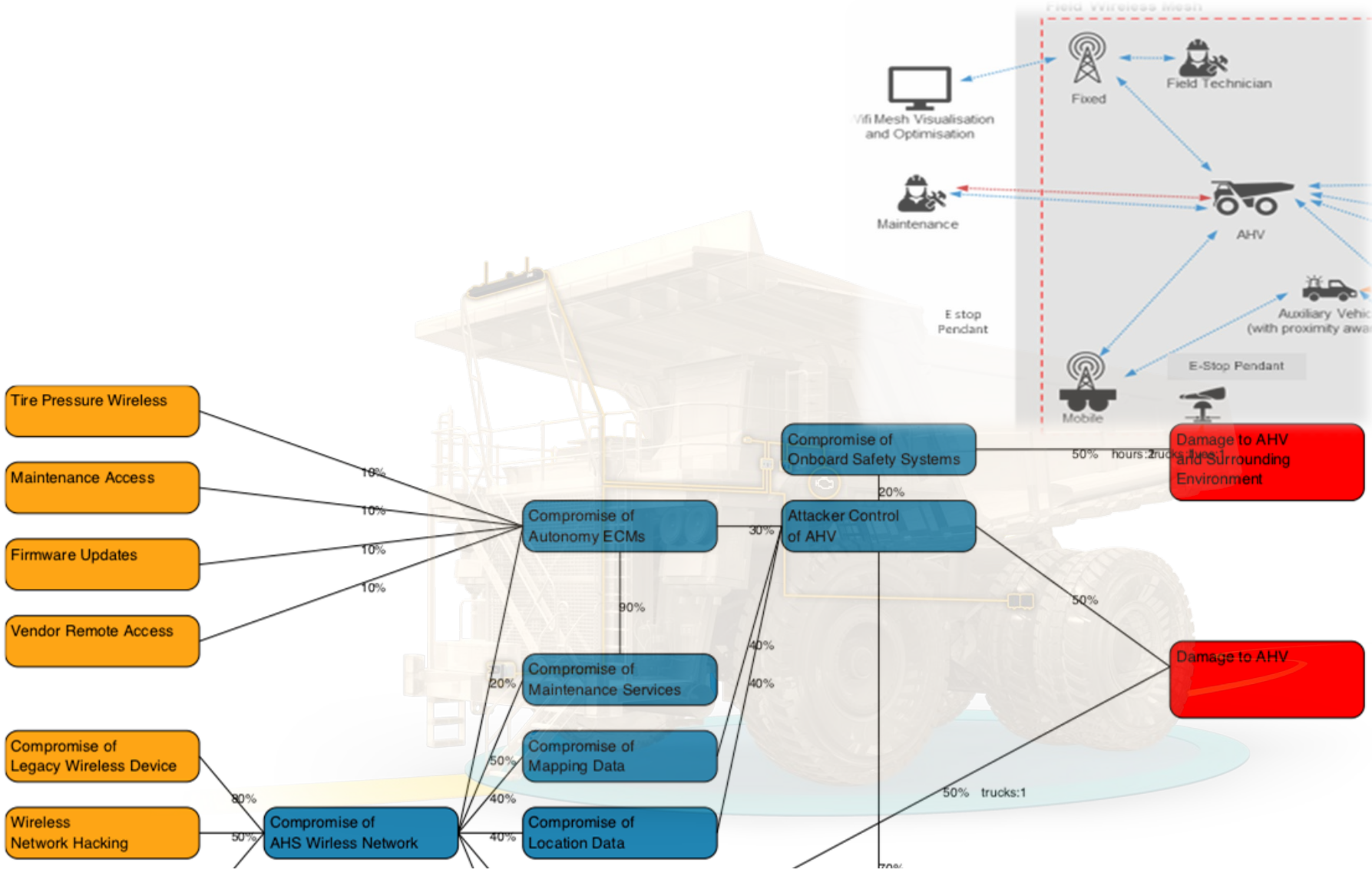
5. HOW TO SECURE AUTONOMOUS HAULAGE SYSTEMS

Securing autonomous haulage systems comes down to understanding the risk relationships between operational assets used in the mining process and autonomous systems on which the processes are dependent. These dependencies can form potential safety, production, and regulatory compliance impacts and risks.

Establishing good risk management practices—including security requirements when new technology is introduced—is crucial to securing autonomous haulage systems effectively. The five following risk management concepts are used for securing autonomous haulage systems:

- Establishing impact: Understand mining process dependencies on OT and the probable loss that could occur if the dependent OT were unavailable.
- Vulnerabilities: Inventory potential attack pathways and system exposure.
- Threats: Conduct threat modelling.
- Assessing Risk: Establish the likelihood (frequency) of a threat exploiting documented vulnerabilities.
- Risk Treatment: Accept assessed risks or mitigate and apply controls.

See Figure 3 for a conceptualization of the risk management processes.


Fixed
Field Technician
Wifi Mesh Visualisation and Optimisation
Maintenance
AHV
E stop Pendant
Auxiliary Vehic
(with proximity awar
E-Stop Pendant
Mobile
Tire Pressure Wireless
Maintenance Access
Firmware Updates
Vendor Remote Access
Compromise of Legacy Wireless Device
Wireless Network Hacking
Compromise of AHS Wirless Network
Compromise of Autonomy ECMs
Compromise of Maintenance Services
Compromise of Mapping Data
Compromise of Location Data
Compromise of Onboard Safety Systems
Attacker Control of AHV
Damage to AHV and Surrounding Environment
Damage to AHV
10%
10%
10%
10%
80%
50%
90%
20%
50%
40%
30%
40%
40%
20%
50%
50%
50% hours:2
50% trucks:1

6. AUTONOMOUS HAULAGE SYSTEM CONTROLS

The MM-ISAC Working Group has created a risk assessment process for members that is complete with controls and mitigation guidance to help with the design process. Some of the key controls are described below.

6.1 OT–IT Integration

Transforming an organization through OT and IT together is key to making OT projects secure and autonomous haulage systems sustainable. Utilizing IT can allow for standardized security control delivery with better availability and effectiveness than if, for example, a process control engineer is trying to run an active directory domain when it can be done more effectively by IT personnel. Key principles with OT–IT integration include:

- It can help maintain secure autonomous haulage system deployment.
- Trained digital forensics and incident response (DFIR) teams can respond to incidents in OT, thereby improving detection and response.
- It can enable opportunities to introduce enterprise governance processes.
- Many components of an OT environment use IT commodity technologies (active directory [AD], backups, remote access, authentication, authorization, and accounting ([AAA]).

6.2 Third Party/OEM

Engaging with potential OEMs before the first contract is signed or pilot is conducted is critical for the success of securing an autonomous haulage system deployment. The required infrastructure configurations are typically certified by the OEMs, which can affect which controls are deployed or what can be patched.

Supply chain security risk is another factor to consider with OEMs and third parties because many maintenance and support personnel are typically required to access critical infrastructure at the mine site, likely requiring their own technology (e.g., laptops). Awareness is crucial to mitigate the requirements of dealing with potential risks after they occur.

6.3 Segmentation

Traditionally, OEMs and vendors have created operational technology without all forms of security controls, referred to as “insecure by design”. Segmentation is one of the only key technical controls for OT that reduces the exposure of OT assets from external untrusted networks. Vendor and OEM roadmaps are in place to fix some of these insecurities in communication protocols, but in the meantime, segmentation is the only form of security for these technologies.

Industrial segmentation standards like the IEC 62443 zones and conduits model or the Purdue reference model are suitable for use in autonomous haulage system environments.

6.4 Access and Authorization

Access and authorization controls and logical network communication form the authentication boundary. The OT perimeter formed by the firewalls also acts as an authentication boundary at the same time.

Secure remote access should be used for all systems that are external to autonomous haulage systems. This means that the authentication boundary should form a perimeter that can only be entered if there is the use of multifactor authentication and secure remote access.

Additionally, when setting up secure remote access, it is recommended to avoid the use of traditional virtual private networks (VPNs) and to take the time to set up jump servers using secure remote access and a secure remote access technology to broker access into the OT. Additional controls such as remote access session recording can be added, allowing forensic analysis if something goes wrong (operational or security incident).

Additional considerations with this control include:

- Separate active directory domain for OT to limit credential theft and privilege escalation attacks
- Enable accounting controls such as log forwarding
- Modern identity features on next-generation firewalls to help limit access to least privilege levels

6.5 Wireless

Autonomous haulage systems require constant communications with their control servers and therefore require increased wireless availability and GPS accuracy in order to be successful.

If there is a loss of communication, the vehicle and any other vehicles in its proximity come to a complete stop. It does not take long for these communications losses to escalate into entire fleet-wide outages that bring the mine production to a standstill.

Securing these wireless networks can be challenging, especially within their constraints. The addition of poorly managed or unsecured wireless networks can render segmentation designs irrelevant.

Wireless de-authentication and disassociation attacks are possible; however, after testing was completed, management frame protection (MFP) that is present on most modern wireless gear was found to mitigate and protect from these attacks. Enabling wireless intrusion capabilities in all network gear and getting them to forward logs to the security information and event manager (SIEM) is a best practice that should be considered.

If the noise floor is raised on the frequencies in or around a GPS, there is a potential to stop autonomous haul trucks. GPS-based jamming attacks have a low barrier-to-entry as an attack vector because GPS noise generators are relatively easy to acquire, which makes attacks more likely. If these attacks do occur, it can be difficult to find the transmitter and require significant amounts of time to locate it using specialized radio gear and trained wireless personnel.

A key control to mitigate these risks is to implement a physical boundary around the autonomous operating zone of the mine. The larger the boundary, the farther the attacker would need to be from the target autonomous vehicles, thereby making raising the noise floor more difficult by causing the

attacker to require a powerful jamming unit to cause a production impact. More advanced mitigations are available; however, they are typically marketed to military agencies.

6.6 Vulnerability Management and Endpoint Protection

Because unknowns can't be secured, ensuring all autonomous haulage system assets are documented and managed in a relevant ITSM/change management platform is mandatory. These asset databases could be used to record business impact information and service risks and dependencies between assets.

Vulnerability management within OT can seem different than IT. In OT, any activity that could lead to an impact on operational availability should be avoided. Active vulnerability scanning, automated patching, and upgrading of hardware and software are not typically permitted, and any disruptive changes or actions required should be tested and work plans approved by relevant mine management. These tasks should be scheduled and completed during a maintenance production outage. Vendors often lock certain hardware and software when patching and updating is required and agreed upon with OEMs and vendors in service and support agreements.

7. SECURING THE MINE OF THE FUTURE

In the past few years, there has been a steep change in new technology adoption used within the mining industry. Many successful autonomous haulage system implementations across the globe have paved the way for a new vision in mining where personnel are removed from the safety risks of working directly within an active mining environment, eliminating operator collisions, or falling asleep at the wheel. OEMs are beginning to offer autonomous options and technologies that could be used in autonomous operations, including:

- Rock drills used in the blasting process
- Blasting trucks that load the explosive emulsion mixture into blast holes
- Tele-remote options (becoming more readily available) for auxiliary equipment such as dozer and excavators

This vision improves personnel safety and certain operational efficiencies. However, as discussed above, this vision also introduces new cybersecurity challenges in managing data, sensors, controls, and securing wireless networks.

Please note that case studies published through GMG are examples of participants' experiences and are not intended to reflect the views of GMG and its members.

About GMG

The Global Mining Guidelines Group (GMG) is a not-for-profit membership organization that brings the global mining community together by providing a platform for collaboration. This open and inclusive hub for innovators to gather facilitates and mobilizes the sharing of knowledge, expertise, and experience to develop operator-driven guidance, resources, and common practices that can be operationalized in response to some of the industry's most pressing demands across the globe

About the MM-ISAC

The Mining and Metals ISAC (MM-ISAC) is a non-profit, industry-owned corporation established to improve the cyber security of metals and mining companies. Its goal is to protect members against incidents that could impact safety, environmental sustainability, or operational productivity. This mission will be achieved by sharing threat and vulnerability information, managing industry contingency planning, providing opportunities for training security staff and incident response teams and innovations. Learn more about GMG at https://gmggroup.org/